TRICARE Management Activity (TMA) Standard Contract Language

2008 Data Protection Seminar

TMA Privacy Office

Contract Language
Purpose

- ☐ Provide an overview of various pieces of contract language used by TMA, including language for the Health Insurance Portability and Accountability Act (HIPAA), Privacy Impact Assessments (PIA), System of Records (SOR), and contractor access to the HA/TMA Network

- ☐ Review Data Use Agreements (DUA)

Contract Language
Objectives

- This presentation will:

  - Explain how contract language protects TMA

  - Identify the impact of inappropriate contract language

  - Describe contract language for:

    - HIPAA

    - Privacy Impact Assessments

    - Contractor Access to the HA/TMA Network

Contract Language

Why Do We Need Contract Language?

- We use contract language to ensure that contractors understand their responsibility in protecting the health information of TRICARE beneficiaries

- Contractors must follow the same privacy and security regulations as government entities

- Contractors can be held accountable for misuse or mishandling of Protected Health Information (PHI) and Personally Identifiable Information (PII)

Contract Language

Impact of Insufficient Non-Purchased Care Contract Language

□ MCA must ensure that appropriate contract language is used by contractors

□ Inappropriate contract language can affect areas such as:

- HIPAA complaints
- Privacy Act compliance
- PHI disclosures
- Data breaches

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA and Contract Language

- ☐ HIPAA requires that contract language be included in agreements between a covered entity and an individual or organization that uses or discloses PHI on behalf of the covered entity, known as the Business Associate (BA)

- ☐ HIPAA Privacy/Security rules require a covered entity to impose contractually safeguards for PHI on persons or entities who work with PHI on behalf of a covered entity

- ☐ Requirement of the BA to safeguard PHI is contractual and HIPAA does not pass through to the BA

HIPAA and Contract Language

- □ HIPAA contract language
  - Requires training for the contractor workforce
  - Requires management and mitigation of complaints
  - Authorizes sanctions for inappropriate activities which could include termination of a contract

HIPAA and Contract Language

- A covered entity may disclose PHI and PII to a contractor if the covered entity obtains satisfactory assurances from the contractor that:

  - The contractor will only use information for the purposes for which the contractor was engaged by the covered entity

  - The contractor will safeguard the information from misuse

  - The contractor will help the covered entity comply with some of the covered entities duties

9

Contract Language

HIPAA and Contract Language

- ☐ If a contract is required, ensure that the TMA "HIPAA Privacy and Security Business Associate Contract Language" is incorporated into your contract

Privacy Impact Assessments (PIA)

Contract Language

PIAs and Contract Language

- Contract language provides for the completion of a PIA for any applicable system that maintains PII on TRICARE beneficiaries

- Caveat: Prior evaluation of the system

System of Records (SOR)

Contract Language

SORs and Contract Language

□ For contracts requiring the maintenance or operation of a System of Records Notice (SORN):

 ■ Contractor will assist with identification of a current SORN or

 ■ Contractor shall assist in completing a SOR for collections of 10 or more records where information is **retrieved** by an identifier

Data Use Agreements (DUA)

DUAs and Contract Language

- DUAs hold those who request data from TMA and MHS accountable for protecting that data

- DUAs are reviewed yearly to ensure continued compliance

- When applying for access to a particular IT system, Account Authorization Request Forms (AARF) hold contractors to the same standards as government employees

Personnel Security

Contract Language

Personnel Security and Contract Language

- Contractor personnel accessing DoD IT systems are subject to Automated Data Processing/Information Technology trustworthiness determinations (ADP/IT-I or ADP/IT-II)

- The contractor workforce must fulfill Information Assurance (IA) training requirements before accessing DoD IT systems

- Contract language ensures consistency in the level of background investigation and IA training

Contract Language
Templates

- The three types of contract language are:

  - PII/PHI

  - Business Associate Agreement (BAA)

  - Contractor access to HA/TMA Network

- Templates are available on the TMA Privacy Office website

- Click on the appropriate link, and copy and paste the language into the contract document

PII/PHI Contract Language

- There are four sections within the PII/PHI Contract Language template:

  - HIPAA

  - PIA

  - SOR

  - DUA

- Use one or all

Contract Language
PII/PHI Contract Language Requirements

- ☐ If the contractor uses any element of PHI in any form, include HIPAA contract language

- ☐ If records are collected, stored, or disseminated with PII and the contractor is using the data for a secondary purpose, include the PIA contract language

- ☐ If records are retrieved by an identifier, include SOR contract language

BAA Contract Language

- BAA Standard Contract Clause

- Use the decision trees to determine applicability

- When in doubt – **ask**

  - PrivacyMail@tma.osd.mil
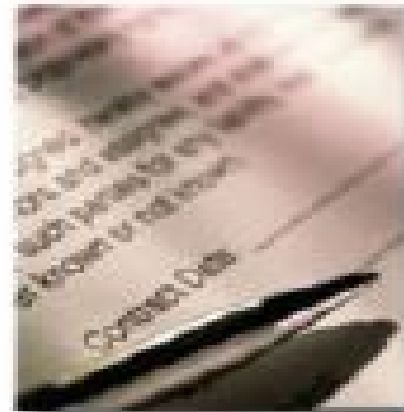
Contractor Access to HA/TMA Network

□ Contractor Access language is mandatory whenever a contractor employee will access the HA/TMA Network or a Department of Defense (DoD) IT system

Contract Language
Summary

- You now can:

  - Explain how contract language protects TMA

  - Identify the impact of insufficient contract language

  - Describe contract language for:

    - HIPAA

    - Privacy Impact Assessments

    - Contractor Access to the HA/TMA Network